

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-344546
(P2001-344546A)

(43) 公開日 平成13年12月14日 (2001. 12. 14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 17/60	4 1 6	G 0 6 F 17/60	4 1 6
	2 2 2		2 2 2
	4 1 4		4 1 4
	5 0 2		5 0 2
	5 0 6		5 0 6

審査請求 未請求 請求項の数12 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願2001-96967(P2001-96967)

(22) 出願日 平成13年3月29日 (2001. 3. 29)

(31) 優先権主張番号 特願2000-90291(P2000-90291)

(32) 優先日 平成12年3月29日 (2000. 3. 29)

(33) 優先権主張国 日本 (J P)

(71) 出願人 300018884

熊坂 憲二

東京都世田谷区八幡山3丁目33番1号 林
マンション304

(72) 発明者 熊坂 憲二

東京都世田谷区八幡山3丁目33番1号 林
マンション304

(74) 代理人 100097113

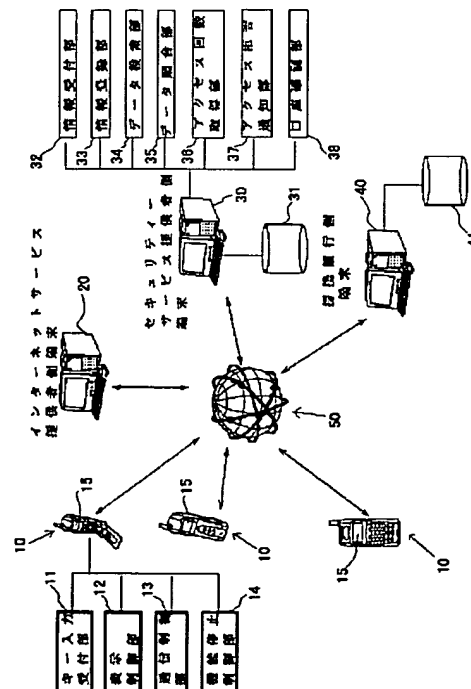
弁理士 堀 城之

(54) 【発明の名称】 携帯情報端末の不正使用防止方法及び記録媒体

(57) 【要約】

【課題】 携帯情報端末の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができるようにする。

【解決手段】 インターネットサービス提供者側端末20がユーザーからの要求により情報提供サービスを行うとき、セキュリティサービス提供者側端末30がユーザーに関する利用者情報とパスワードとを加入者データベース31から参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末40がユーザーの銀行口座の残高を示す情報を口座情報データベース41から参照してセキュリティサービス提供者側端末30に与えるようにする。



【特許請求の範囲】

【請求項1】 ユーザーが携帯情報端末を用いて情報提供サービスを受ける第1の工程と、

インターネットサービス提供者側端末が前記携帯情報端末からの要求により前記情報提供サービスを行う第2の工程と、

前記インターネットサービス提供者側端末からの依頼により、セキュリティサービス提供者側端末が前記ユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、前記インターネットサービス提供者側端末による前記情報提供サービスを許可する第3の工程と、前記情報提供サービスが決済を伴うとき、セキュリティサービス提供者側端末からの依頼により、提携銀行側端末が前記ユーザーの銀行口座の残高を示す情報を口座情報データベースから参照して前記セキュリティサービス提供者側端末に与える第4の工程とを備えることを特徴とする携帯情報端末の不正使用防止方法。

【請求項2】 前記第1の工程には、前記加入者データベースに登録するための利用者情報とパスワードとを送信する第5の工程と、

決済を伴う前記情報提供サービスを受けるとき、前記利用者情報とパスワードとを送信する第6の工程とが含まれ、

前記第2の工程には、前記利用者情報とパスワードとを受取ると、これらの情報を前記セキュリティサービス提供者側端末に送信する第7の工程が含まれ、

前記第3の工程には、前記正規のユーザーであることが確認できたとき、直ちに前記銀行口座の残高を調べ、引き落としが可能かどうかを前記インターネットサービス提供者側端末を介して前記ユーザーに通知する第8の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項3】 前記第3の工程には、データ照合部により、前記加入者データベースから参照したデータが一致しないとき、正規のユーザーでないことを前記インターネットサービス提供者側端末に通知する第9の工程が含まれ、

前記第2の工程には、前記正規のユーザーでないことの通知を受けると、前記ユーザーのアクセスを拒否する第10の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項4】 前記第9の工程には、アクセス回数取得部により、前記ユーザーのアクセス拒否の回数と前記ユーザーの利用者情報とを保持し、一定回数以上のアクセス拒否が起きると、前記インターネットサービス提供者側端末に通知する第11の工程が含まれることを特徴とする請求項3に記載の携帯情報端末の不正使用防止方法。

【請求項5】 前記第1の工程には、正規のユーザーで

あることが確認された後、決済の意志を前記インターネットサービス提供者側端末に送信する第12の工程が含まれ、

前記第2の工程には、前記ユーザーからの決済の意志を前記セキュリティサービス提供者側端末に送信する第13の工程が含まれ、

前記第3の工程には、口座確認部により、前記提携銀行側端末へ前記ユーザーの銀行口座からの代金の引き落としが可能かどうかを確認するための要求を行う第14の工程が含まれ、

前記第4の工程には、前記引き落としが可能かどうかを調べた結果を前記セキュリティサービス提供者側端末に送信する第15の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項6】 前記第12の工程には、前記引き落としが可能であるとき、決済の最終確認を前記インターネットサービス提供者側端末に通知する第16の工程が含まれ、

前記第13の工程には、前記セキュリティサービス提供者側端末に引き落としの依頼を通知する第17の工程が含まれ、

前記第14の工程には、前記提携銀行側端末に引き落としの依頼を通知する第18の工程が含まれ、

前記第15の工程には、前記セキュリティサービス提供者側端末に引き落としの完了を通知する第19の工程が含まれることを特徴とする請求項5に記載の携帯情報端末の不正使用防止方法。

【請求項7】 前記第18の工程には、前記インターネットサービス提供者側端末に引き落としの完了を通知する第20の工程が含まれ、

前記第17の工程には、前記携帯情報端末に引き落としの完了を通知する第21の工程が含まれることを特徴とする請求項6に記載の携帯情報端末の不正使用防止方法。

【請求項8】 前記利用者情報は、前記ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号であることを特徴とする請求項1、2又は4に記載の携帯情報端末の不正使用防止方法。

【請求項9】 前記利用者情報は、特定の文字列であることを特徴とする請求項1、2又は4に記載の携帯情報端末の不正使用防止方法。

【請求項10】 請求項1～9の何れかに記載の携帯情報端末の不正使用防止方法を実行可能なプログラムが記録されていることを特徴とする記録媒体。

【請求項11】 コンピュータに第1の工程～第4の工程を実行させるためのプログラム。

【請求項12】 コンピュータに第1の工程～第21の工程を実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話やノートパソコン等の携帯情報端末の使用者が正規の使用者であるか否かを特定して不正使用を防止したりオンラインショッピングなどの決済を行ったりする携帯情報端末の不正使用防止方法及び記録媒体に関する。

【0002】

【従来の技術】近年、携帯電話やノートパソコン等の携帯情報端末が普及している。これらは、使用する場所等が特定されないばかりか、たとえばインターネットを気軽に利用することができるようになっている。さらに、インターネットを用いてのオンラインショッピングの決済なども手軽に行われるようになってい

【0003】

【発明が解決しようとする課題】ところで、上述した携帯電話やノートパソコン等の携帯情報端末の普及に伴い、紛失や盗難等の発生が増えている。これら携帯電話やノートパソコン等の携帯情報端末は、たとえば暗唱番号等を用いてのキーロック操作を行うことで、第三者の使用を防止できるようになっている。

【0004】ところが、使い勝手の面から暗唱番号等を用いてのキーロック操作を行う場合が少なく、たとえキーロック操作を行っても暗唱番号の解読等により、不正使用されてしまうことがある。このように、不正使用されると、たとえばオンラインショッピングの決済なども第三者によって行われることが予測され、正規の使用者が被害を被ることもあり得る。

【0005】このため、携帯電話やノートパソコン等の携帯情報端末の不正使用を確実に防止することができるシステムの開発が望まれている。

【0006】本発明は、このような状況に鑑みてなされたものであり、携帯情報端末の使用者が正規の使用者であるか否かを特定することで、不正使用を防止することができる携帯情報端末の不正使用防止方法及び記録媒体を提供することができるようにするものである。

【0007】

【課題を解決するための手段】請求項1に記載の携帯情報端末の不正使用防止方法は、ユーザーが携帯情報端末を用いて情報提供サービスを受ける第1の工程と、インターネットサービス提供者側端末が携帯情報端末からの要求により情報提供サービスを行う第2の工程と、インターネットサービス提供者側端末からの依頼により、セキュリティサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、インターネットサービス提供者側端末による情報提供サービスを許可する第3の工程と、情報提供サービスが決済を伴うとき、セキュリティサービス提供者側端末からの依頼により、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティサービス提供者側端末に与える第4の工

程とを備えることを特徴とする。また、第1の工程には、加入者データベースに登録するための利用者情報とパスワードとを送信する第5の工程と、決済を伴う情報提供サービスを受けるとき、利用者情報とパスワードとを送信する第6の工程とが含まれ、第2の工程には、利用者情報とパスワードとを受取ると、これらの情報をセキュリティサービス提供者側端末に送信する第7の工程が含まれ、第3の工程には、正規のユーザーであることが確認できたとき、直ちに銀行口座の残高を調べ、引き落としが可能かどうかをインターネットサービス提供者側端末を介してユーザーに通知する第8の工程が含まれるようにすることができる。また、第3の工程には、データ照合部により、加入者データベースから参照したデータが一致しないとき、正規のユーザーでないことをインターネットサービス提供者側端末に通知する第9の工程が含まれ、第2の工程には、正規のユーザーでないことの通知を受けると、ユーザーのアクセスを拒否する第10の工程が含まれるようにすることができる。また、第9の工程には、アクセス回数取得部により、ユーザーのアクセス拒否の回数とユーザーの利用者情報とを保持し、一定回数以上のアクセス拒否が起きると、インターネットサービス提供者側端末に通知する第11の工程が含まれるようにすることができる。また、第1の工程には、正規のユーザーであることが確認された後、決済の意志をインターネットサービス提供者側端末に送信する第12の工程が含まれ、第2の工程には、ユーザーからの決済の意志をセキュリティサービス提供者側端末に送信する第13の工程が含まれ、第3の工程には、口座確認部により、提携銀行側端末へユーザーの銀行口座からの代金の引き落としが可能かどうかを確認するための要求を行う第14の工程が含まれ、第4の工程には、引き落としが可能かどうかを調べた結果をセキュリティサービス提供者側端末に送信する第15の工程が含まれるようにすることができる。また、第12の工程には、引き落としが可能であるとき、決済の最終確認をインターネットサービス提供者側端末に通知する第16の工程が含まれ、第13の工程には、セキュリティサービス提供者側端末に引き落としの依頼を通知する第17の工程が含まれ、第14の工程には、提携銀行側端末に引き落としの依頼を通知する第18の工程が含まれ、第15の工程には、セキュリティサービス提供者側端末に引き落としの完了を通知する第19の工程が含まれるようにすることができる。また、第18の工程には、インターネットサービス提供者側端末に引き落としの完了を通知する第20の工程が含まれ、第17の工程には、携帯情報端末に引き落としの完了を通知する第21の工程が含まれるようにすることができる。また、利用者情報は、ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号であるようにすることができる。また、利用者情報は、特定の文字列であるようにす

ることができる。請求項10に記載の記録媒体は、請求項1～9の何れかに記載の携帯情報端末の不正使用防止方法を実行可能なプログラムが記録されていることを特徴とする。請求項11に記載のプログラムは、コンピュータに第1の工程～第4の工程を実行させる。請求項12に記載のプログラムは、コンピュータに第1の工程～第21の工程を実行させる。本発明に係る携帯情報端末の不正使用防止方法及び記録媒体においては、インターネットサービス提供者側端末がユーザーからの要求により情報提供サービスを行うとき、セキュリティサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティサービス提供者側端末に与えるようにする。

【0008】

【発明の実施の形態】以下、本発明の実施の形態について説明する。図1は、本発明の携帯情報端末の不正使用防止方法の一実施の形態に係る不正使用防止システムの概要を示す図、図2は、図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図、図3及び図4は、図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャート、図5～図10は、図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【0009】図1に示す不正使用防止システムは、一般ユーザーが使用する携帯情報端末10、インターネットサービス提供者側端末20、セキュリティサービス提供者側端末30及び提携銀行側端末40を備え、これらはインターネット50を介して相互に通信できるようになっている。

【0010】携帯情報端末10は、たとえば携帯電話、ノートパソコン、PDA（個人情報端末）等の携帯型の通信手段である。携帯情報端末10は、キー入力受付部11、表示制御部12、通信制御部13、機能停止制御部14を備えている。キー入力受付部11は、携帯情報端末10のキーからの入力を受付けるものである。

【0011】表示制御部12は、ディスプレイ15への情報表示を制御するものである。通信制御部13は、インターネット50を介しての通信を制御するものである。機能停止制御部14は、一定回数以上のアクセス拒否が起きると、セキュリティサービス提供者側端末30からの制御により、機能を停止させるものであり、その詳細は後述する。

【0012】インターネットサービス提供者側端末20は、オンラインショッピング等のサービスを提供するものである。セキュリティサービス提供者側端末30

は、携帯情報端末10の不正使用を防止したりするものであり、加入者データベース31、情報受付部32、情報登録部33、データ検索部34、データ照合部35、アクセス回数取得部36、アクセス拒否通知部37、口座確認部38を備えている。

【0013】加入者データベース31には、携帯情報端末10の利用者情報とパスワードとが登録されるようになっている。ここで、利用者情報としては、一般ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号などである。また、これらの情報以外に、たとえばユーザーが指定した特定の文字列なども利用者情報として用いることができる。ここで、特定の文字列とは、たとえば好きな言葉であったり、詞であったり、歌詞であったり、何か意味をもつ内容であったりしてもよい。何れにしても、ユーザー個人のみが知り得るものであればよい。

【0014】情報受付部32は、携帯情報端末10からの利用者情報やパスワードなどを受付けるものである。情報登録部33は、受付けた利用者情報やパスワードなどを加入者データベース31に登録するものである。

【0015】データ検索部34は、携帯情報端末10からのアクセスに応じて加入者データベース31に登録されているデータを検索するものである。データ照合部35は、データ検索部34によって検索されたデータの照合を行うものであり、データの照合が一致すると、正規のユーザーであると判断される。アクセス回数取得部36は、データ照合部35によるデータの照合の不一致に応じた携帯情報端末10からのアクセス回数を取得するものである。

【0016】アクセス拒否通知部37は、アクセス回数取得部36によるデータの照合の不一致のアクセスが一定回数以上であるとき、携帯情報端末10側へ機能停止のための制御信号を送信する。このとき、携帯情報端末10側では、機能停止制御部14により、通信機能が停止される。また、携帯情報端末10側の機能停止を行わせる場合、インターネットサービス提供者側端末20へ機能停止のための制御信号を送信し、インターネットサービス提供者側端末20からの通信キャリアの送信を停止させるようにすることもできる。口座確認部38は、携帯情報端末10からの決済の要求が生じたとき、提携銀行側端末40の口座の残高を調べ、引き落としが可能かどうかを確認するものである。提携銀行側端末40は、口座情報データベース41を備えている。口座情報データベース41は、ユーザーの銀行口座の残高などを管理するものである。

【0017】次に、このような不正使用防止システムにおける携帯情報端末の不正使用防止方法の概要について説明する。

【0018】まず、図2中の(1)は、ユーザーがたとえばオンラインショッピングなどの決済を必要とするサ

ービスを提供しているインターネットサイトにアクセスして、物品の購入などを行い決済の意志を伝えることを示す。このアクセスの際は、予め加入者データベース31に登録してある利用者情報とパスワードとを入力する。

【0019】これにより、利用者情報は一意であり、重複する番号はなく、パスワードは本人しか知り得ない情報であるため、アクセスしている人物が、正規のユーザーであるかどうかの判断ができる。

【0020】図2中の(2)は、インターネットサービス提供者が(1)で入力された利用者情報とパスワードとをセキュリティサービス提供者に送信することを示す。図2中の(3)は、セキュリティサービス提供者が(2)で受信したデータを使って、予め登録されている加入者データベース31を検索し、照合を行い、その結果を、インターネットサービス提供者に送信することを示す。

【0021】図2中の(4)は、インターネットサービス提供者が(3)で受信したデータを(1)でアクセスしてきたユーザーに送信することを示す。つまりここで、正規のユーザーであれば、予め登録してある氏名、住所、年齢、電話番号、銀行口座番号が表示されて確認をすることができる。正規のユーザーでなければ、アクセスが拒否された旨のメッセージが表示され、決済の処理が中止される。

【0022】このとき、セキュリティサービス提供者では、アクセスが拒否された利用者情報とその回数を記録しておき、一定回数以上のアクセス拒否が起きると、その利用者情報を使用できなくするようにでき、安全性が高められる。同時に、登録されている氏名、住所宛てに郵送で利用者情報が使えなくなったことを伝えるようにすることができる。

【0023】図2中の(5)は、正規のユーザーであることが確認されたので再度、決済の意志をインターネットサービス提供者に送信することを示す。図2中の(6)は、インターネットサービス提供者がセキュリティサービス提供者に(5)で受信したデータを送信することを示す。

【0024】図2中の(7)は、セキュリティサービス提供者から、提携銀行へ(4)で認証されたユーザーの予め登録されている銀行口座から代金の引き落としが可能かどうかを確認することを示す。図2中の(8)は、提携銀行からセキュリティサービス提供者へ引き落としが可能かどうかを調べた結果を送信することを示す。

【0025】図2中の(9)は、セキュリティサービス提供者からインターネットサービス提供者へ(8)の情報を送信することを示す。図2中の(10)は、インターネットサービス提供者からユーザーへ(8)の結果を送信することを示す。つまりここで、引き落としが可

能であれば次のステップへ進むことができる。引き落としが不可能であれば、その旨のメッセージが表示され、決済の処理が中止される。

【0026】図2中の(11)は、引き落としが可能であるため、決済の最終確認を行い、ユーザーの決済の意志をインターネットサービス提供者に送信することを示す。図2中の(12)は、インターネットサービス提供者がセキュリティサービス提供者に引き落としの依頼を送信することを示す。

10 【0027】図2中の(13)は、セキュリティサービス提供者が提携銀行に引き落としの依頼を送信することを示す。図2中の(14)は、提携銀行がセキュリティサービス提供者に引き落としの完了を送信することを示す。図2中の(15)は、セキュリティサービス提供者がインターネットサービス提供者に引き落としの完了を送信することを示す。図2中の(16)は、インターネットサービス提供者がユーザーに引き落としの完了を送信することを示す。

20 【0028】なお、全ての処理において、インターネット50上を通る情報は暗号化しておく、さらに安全性が高められる。図2中の(2)の処理の後、セキュリティサービス提供者では、正規のユーザーであることが確認できたら、直後に提携銀行の口座の残高を調べ、引き落としが可能かどうかを確認しておき、図2中の(9)の処理に戻るようにすることもできる。また、引き落としして完了した場合、図2中の(15)の処理に戻るようにすることもできる。

30 【0029】次に、このような不正使用防止システムにおける携帯情報端末の不正使用防止方法について説明する。

【0030】まず、携帯情報端末10のユーザーは、予め自分の情報をセキュリティサービス提供者30の加入者データベース31に登録しておく。加入者データベース31に登録される情報は、上述したユーザーの氏名、住所、年齢、電話番号、顧客管理番号、パスワード、銀行口座番号などである。また、上述したように、たとえばユーザーが指定した特定の文字列なども登録しておくことができる。

40 【0031】そして、まず、図3に示すように、ユーザーがたとえばオンラインショッピングなどの決済を必要とするサービスを提供しているインターネットサイトにアクセスする(ステップ201:図2中の(1))。ここで、物品の購入などを行い決済の意志を伝えるためのアクセスの際は、予め加入者データベース31に登録してある利用者情報とパスワードとを入力する。

50 【0032】このとき、携帯情報端末10のディスプレイ15には、たとえば図5に示すような内容が表示される。ここでは、利用者情報とパスワードの入力が促される。ここで、利用者情報とパスワードとを入力して『次へ』を操作すると、それらの情報がインターネットサー

ビス提供者側端末20に送信される。

【0033】これら利用者情報とパスワードとの入力が入力されると(ステップ202)、インターネットサービス提供者側20が図2中の(1)で入力された利用者情報とパスワードとをセキュリティサービス提供者側端末30に送信する(ステップ203:図2中の(2))。

【0034】利用者情報とパスワードとを受けたセキュリティサービス提供者側端末30のデータ検索部34により、図2中の(2)で受信したデータを使って、予め登録されている加入者データベース31が検索されると、データ照合部35により照合が行われ、照合が一致するとその結果が、インターネットサービス提供者側端末20に送信される(ステップ204:図2中の(3))。

【0035】その結果を受けたインターネットサービス提供者側端末20は、図2中の(3)で受信したデータを図2中の(1)でアクセスしてきたユーザーに送信する(ステップ205:図2中の(4))。つまりここで、正規のユーザーであれば(ステップ206)、予め登録してある氏名、住所、年齢、電話番号、銀行口座番号や特定の文字列が表示されて確認をすることができ、これに対し、データ照合部35により照合が不一致である場合、正規のユーザーでないため、アクセスが拒否された旨のメッセージが携帯情報端末10のディスプレイ15に表示され(ステップ207)、決済の処理が中止される。

【0036】このとき、正規のユーザーであると確認されると、携帯情報端末10の画面には、たとえば図6に示すような内容が表示され、その画面で『次へ』を操作すると、次のステップへ進むことができる。また、正規のユーザーでない場合、携帯情報端末10の画面には、たとえば図7に示すような内容が表示される。

【0037】このとき、セキュリティサービス提供者側端末30のアクセス回数取得部36により、アクセスが拒否された利用者情報とその回数が保持され、一定回数以上のアクセス拒否が起きると、アクセス拒否通知部37により、携帯情報端末10側へ機能停止のための制御信号が送信される。このとき、携帯情報端末10側では、機能停止制御部14により、通信機能が停止される。また、携帯情報端末10側の機能停止を行わせる場合、インターネットサービス提供者側端末20へ機能停止のための制御信号を送信し、インターネットサービス提供者側端末20からの通信キャリアの送信を停止させるようにすることもできる。

【0038】これにより、携帯情報端末10の使用が不可能となるため、安全性が高められる。同時に、登録されている氏名、住所宛てに郵送で利用者情報が使えなくなったことを伝えるようにすることができる。

【0039】次いで、ユーザーは、正規のユーザーであることが確認されたので再度、決済の意志をインターネ

ットサービス提供者側端末20に送信する(ステップ208:図2中の(5))。決済の意志を受けたインターネットサービス提供者側端末20は、セキュリティサービス提供者側端末30に図2中の(5)で受信したデータを送信する(ステップ209:図2中の(6))。

【0040】そのデータを受信したセキュリティサービス提供者側端末30は、提携銀行側端末40へ図2中の(4)で認証されたユーザーの予め登録されている銀行口座から代金の引き落としが可能かどうかを確認する(ステップ210:図2中の(7))。提携銀行側端末40は、セキュリティサービス提供者側端末30へ引き落としが可能かどうかを調べた結果を送信する(ステップ211:図2中の(8))。

【0041】引き落としが可能かどうかの結果を受けたセキュリティサービス提供者側端末30は、インターネットサービス提供者側端末20へ図2中の(8)の情報を送信する(ステップ212:図2中の(9))。インターネットサービス提供者側端末20は、ユーザーへ図2中の(8)の結果を送信する(ステップ213:図2中の(10))。

【0042】つまりここで、引き落としが可能であれば次のステップへ進むことができる。引き落としが不可能であれば、その旨のメッセージが表示され、決済の処理が中止される(ステップ214、215)。

【0043】このとき、引き落としが可能であれば、携帯情報端末10のディスプレイ15には、たとえば図8に示すような内容が表示され、その画面で『次へ』を操作すると、次のステップへ進むことができる。また、引き落としが不可能であれば、携帯情報端末10のディスプレイ15には、たとえば図9に示すような内容が表示される。

【0044】次に、図4に示すように、引き落としが可能であると、決済の最終確認を行うために、ユーザーの決済の意志をインターネットサービス提供者側端末20に送信する(ステップ301:図2中の(11))。インターネットサービス提供者側端末20は、セキュリティサービス提供者側端末30に引き落としの依頼を送信する(ステップ302:図2中の(12))。セキュリティサービス提供者側30の口座確認部38は、提携銀行40に引き落としの依頼を送信する(ステップ303:図2中の(13))。提携銀行側端末40は、セキュリティサービス提供者側端末30に引き落としの完了を送信する(ステップ304:図2中の(14))。

【0045】セキュリティサービス提供者側端末30は、インターネットサービス提供者側端末20に引き落としの完了を送信する(ステップ305:図2中の(15))。インターネットサービス提供者側端末20は、ユーザーに引き落としの完了を送信する(ステップ306:図2中の(16))。このとき、携帯情報端末10のディスプレイ15には、たとえば図10に示すような

内容が表示される。

【0046】このように、本実施の形態では、インターネットサービス提供者側端末20がユーザーからの要求により情報提供サービスを行うとき、セキュリティサービス提供者側端末30がユーザーに関する利用者情報とパスワードとを加入者データベース31から参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末40がユーザーの銀行口座の残高を示す情報を口座情報データベース41から参照してセキュリティサービス提供者側端末30に与えるようにしたので、携帯情報端末10の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができる。

【0047】なお、本実施の形態では、オンラインショッピングの決済の場面などにおいて、本人であるかどうかを確認する場合について説明したが、この例に限らず、電話をかける直前、電話の電源を入れた直後なども同様に本人であるかどうかを確認するようにすることができる。

【0048】さらに、セキュリティサービス提供者側端末30は、正規の登録者の情報でない照会が頻繁に起こった場合、通信キャリアを通じて、携帯情報端末10の登録名義人に対して警告（お知らせ）を行うことができる。同時に通信キャリアでは、その携帯情報端末10の使用を停止することもできる。

【0049】なお、全ての処理において、インターネット50上を通る情報は暗号化しておく、さらに安全性が高められる。また、図2中の(2)の処理の後、セキュリティサービス提供者側端末30では、正規のユーザーであることが確認できたら、直後に提携銀行側端末40の口座の残高を調べ、引き落としが可能かどうかを確認しておき、図2中の(9)の処理に戻るようにすることもできる。また、引き落としまで完了した場合、図2中の(15)の処理に戻るようにすることもできる。

【0050】

【発明の効果】以上の如く本発明に係る携帯情報端末の不正使用防止方法及び記録媒体によれば、インターネットサービス提供者側端末がユーザーからの要求により情報提供サービスを行うとき、セキュリティサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティサービス提供者側端末に与えるようにしたので、携帯情報端

末の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができる。

【図面の簡単な説明】

【図1】本発明の携帯情報端末の不正使用防止方法の一実施の形態に係る不正使用防止システムの概要を示す図である。

【図2】図1の不正使用防止システムの概要を示す図である。

【図3】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャートである。

【図4】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャートである。

【図5】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図6】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図7】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図8】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

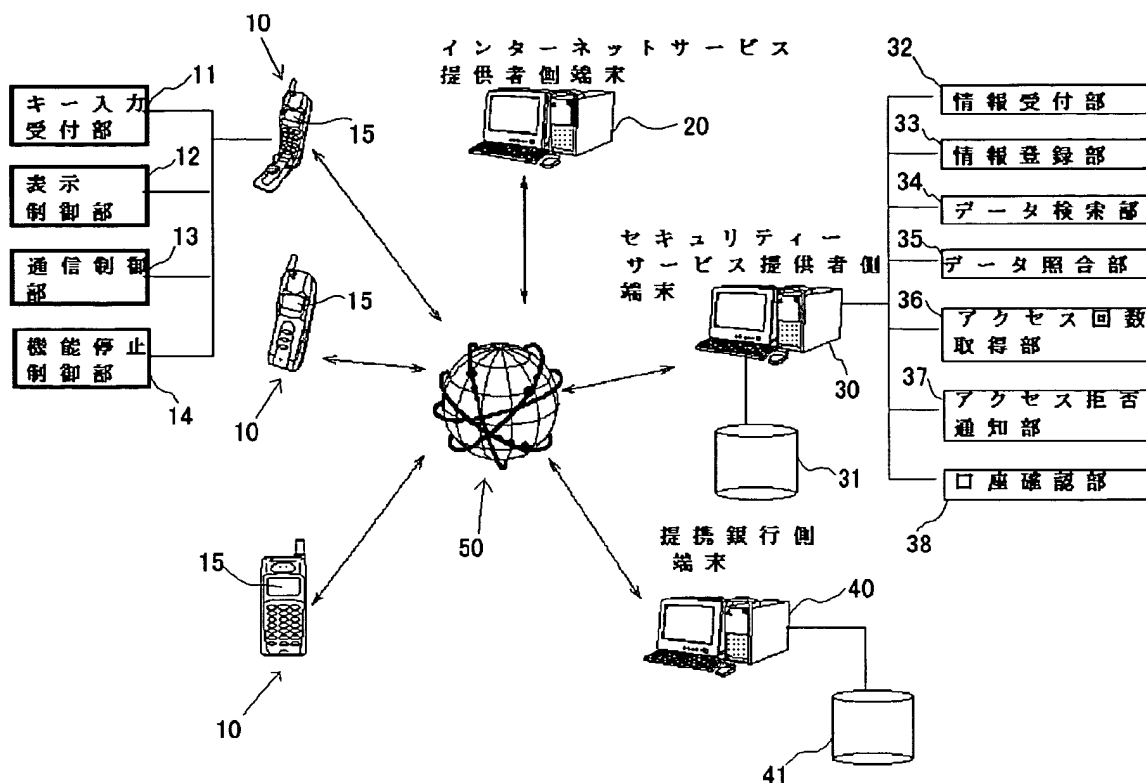
【図9】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図10】図1の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

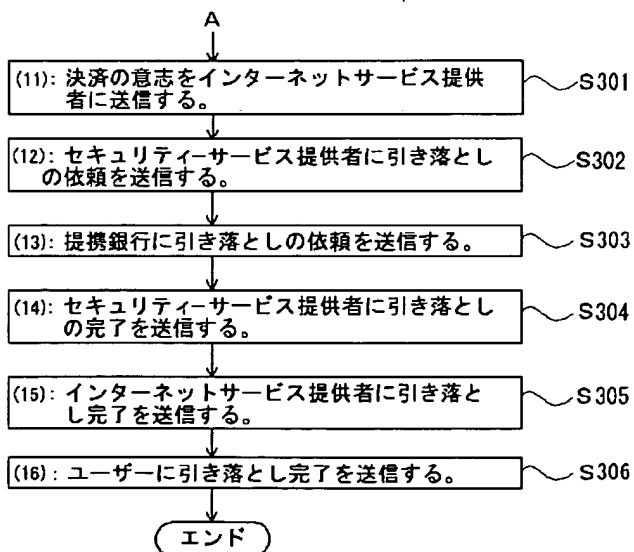
【符号の説明】

- 10 携帯情報端末
- 20 インターネットサービス提供者側端末
- 30 セキュリティサービス提供者側端末
- 31 加入者データベース
- 32 情報受付部
- 33 情報登録部
- 34 データ検索部
- 35 データ照合部
- 36 アクセス回数取得部
- 37 アクセス拒否通知部
- 38 口座確認部
- 40 提携銀行側端末
- 41 口座情報データベース
- 50 インターネット

【図1】



【図4】



【図5】

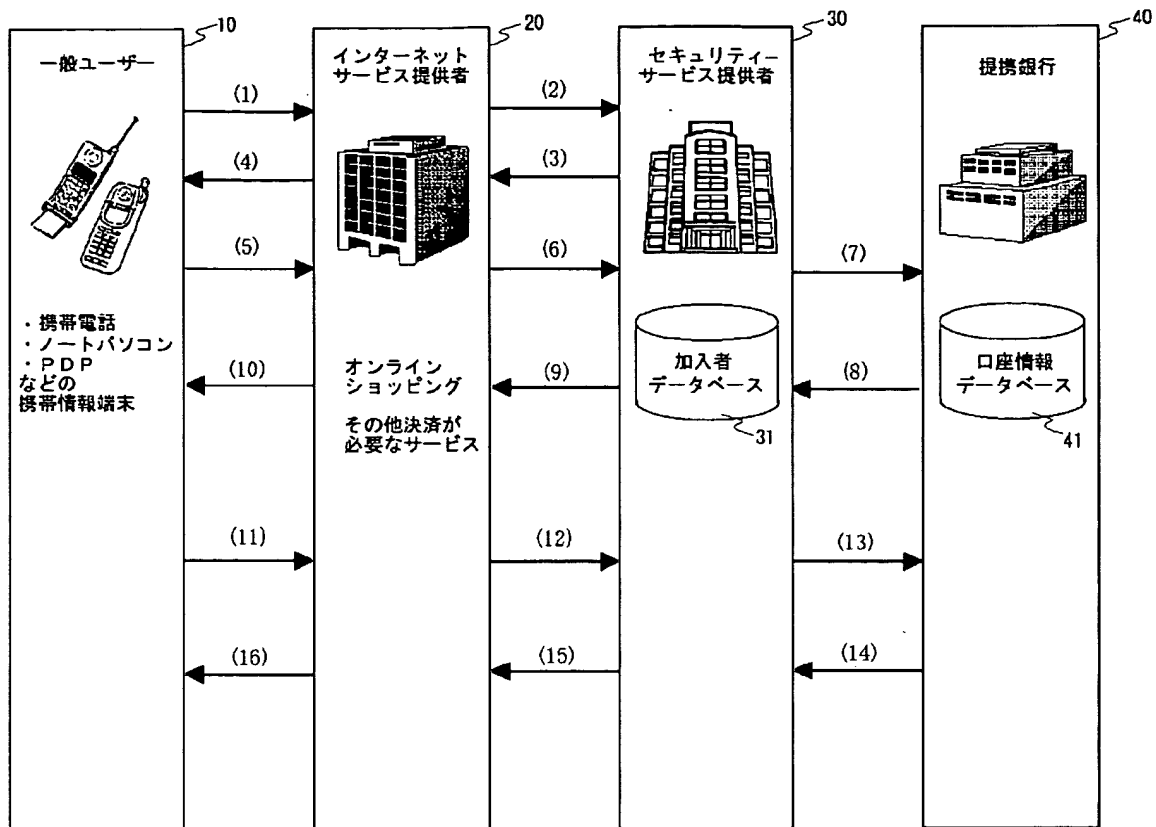
利用者情報入力画面

利用者情報を入力してください

利用者情報 : 090AEPOS01290
パスワード : *****

次へ

【図2】



【図6】

【図7】

照会成功画面

照会成功

入力された利用者情報は承認されました。

次へ

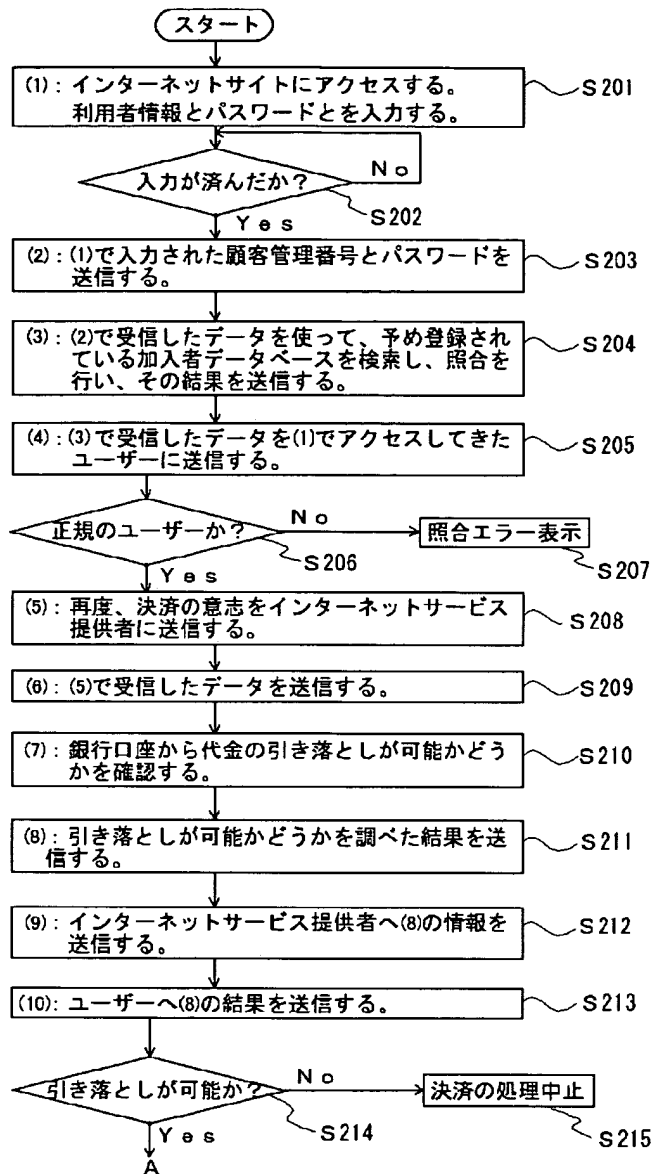
照会エラー画面

照会エラー

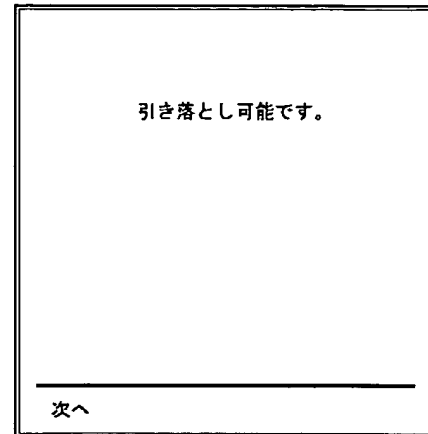
利用者情報が正しくありません。

確認

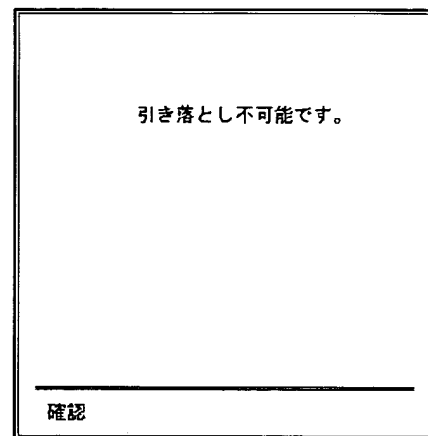
【図3】



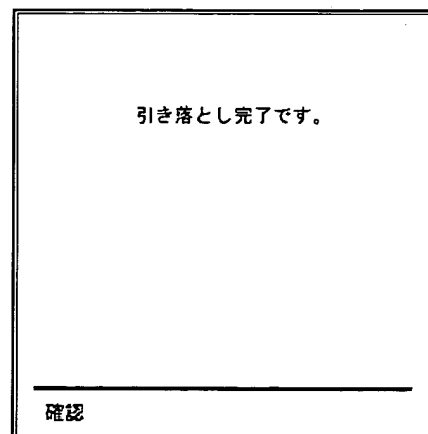
【図8】



【図9】



【図10】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	ターミナル (参考)
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S